ESET MOBILE SECURITY

PARA ANDROID

Guia do Usuário

(destinado ao produto versão 2.0 e posterior)

Clique aqui para fazer download da versão mais recente deste documento

ESET **MOBILE SECURITY**

Atendimento ao Cliente: www.eset.com/support

REV. 23. 8. 2013

Índice

1. Introdução

O ESET Mobile Security é uma solução de segurança completa que protege seu dispositivo contra ameaças emergentes e páginas de phishing, filtra chamadas e mensagens indesejadas e permite que você assuma o controle do seu aparelho remotamente em caso de perda ou roubo.

1.1 O que há de novo

Em comparação com a versão 1.2, as novidades e aprimoramentos a seguir foram introduzidos no ESET Mobile Security versão 2:

Suporte de Tablet
O novo design responde a tablets de forma horizontal e vertical. Alguns recursos (por exemplo Antifurto) ficam ocultos em dispositivos que não suportam as funções de chamadas e mensagens.

Antiphishing
Proteja-se contra sites nocivos tentando adquirir suas informações sensíveis como nomes de usuário, senhas, informações bancárias ou detalhes de cartão de crédito.

Varredura Programada
Agende um rastreamento regular em busca de malware quando for melhor para você, ou mesmo durante a noite, se quiser.

SMS & Filtro de Chamadas com Horário
Bloqueie chamadas e mensagens apenas durante horários específicos, permitindo exceções para família e amigos. Use seus grupos de contato no Android (família, amigos, trabalho) para aplicar regras para cada grupo.

ESET Live Grid
Garanta uma proteção em tempo real contra ameaças emergentes usando a tecnologia na nuvem coletando amostras de malware dos usuários de produtos ESET de todo o mundo.

Alarme remoto
Encontre seu dispositivo ativando um alarme sonoro, mesmo se ele estiver configurado como silencioso.

Detecção de aplicativos potencialmente não desejados
Descubra aplicativos que podem causar danos ao explorar os dados ou funções do seu dispositivo. A detecção prévia protege-o contra tentativas de enviar SMS ou de fazer chamadas para números premium.

Monitoramento do Dispositivo
Verifique se o roaming de chamadas ou dados está ligado, o Wi-Fi no qual você está conectado ou a memória disponível.

Auditoria de Aplicativo
Consulte os níveis de permissão de todos os seus aplicativos instalados - todos eles organizados em grupos. Saiba quais informações do seu dispositivo eles podem acessar.

Novo design
A interface gráfica do usuário, a janela principal do programa e as configurações do programa foram completamente redesenhadas para oferecer uma navegação mais intuitiva e fácil.

1.2 Requisitos do sistema

Para instalar o ESET Mobile Security, seu dispositivo Android deve atender aos requisitos mínimos do sistema a seguir:

Sistema operacional: Android 2.3 (Gingerbread) e versões posteriores
Resolução da tela de toque: no mínimo 240x320 px, recomendado 320x480 px
CPU: 500 MHz
RAM: 256 MB
Espaço de armazenamento interno livre: 12 MB

OBSERVAÇÃO: Dispositivos com root não são suportados. Alguns recursos (por exemplo Antifurto e SMS e Filtro de Chamadas) não estão disponíveis em tablets que não suportam chamadas e mensagens.

2. Instalação

Para instalar o ESET Mobile Security, use um dos métodos a seguir.

OBSERVAÇÃO: Se já possuir um Nome de usuário e Senha ativos ou uma Chave de ativação emitida pela ESET, faça download do ESET Mobile Security a partir do site ESET.

2.1 Instalação do site ESET

Faça download do ESET Mobile Security lendo o código QR a seguir usando seu dispositivo móvel e um aplicativo como QR Droid ou Barcode Scanner:

Alternativamente, é possível fazer download do arquivo de instalação APK do ESET Mobile Security no seu computador:

1. Faça download do arquivo a partir do site da ESET.
2. Copie o arquivo para o seu dispositivo via Bluetooth ou USB.
3. Toque no ícone do iniciador na tela inicial do Android (ou vá para **Início** > **Menu** e toque em **Configurações** > **Aplicativos**. Certifique-se de que **Fontes desconhecidas** está selecionado.
4. Localize o arquivo APK usando um aplicativo de navegação de arquivos como o ASTRO File Manager ou ES File Explorer.
5. Abra o arquivo e toque em **Instalar**. Depois que o aplicativo for instalado, toque em **Abrir**.

2.2 Instalação do Google Play

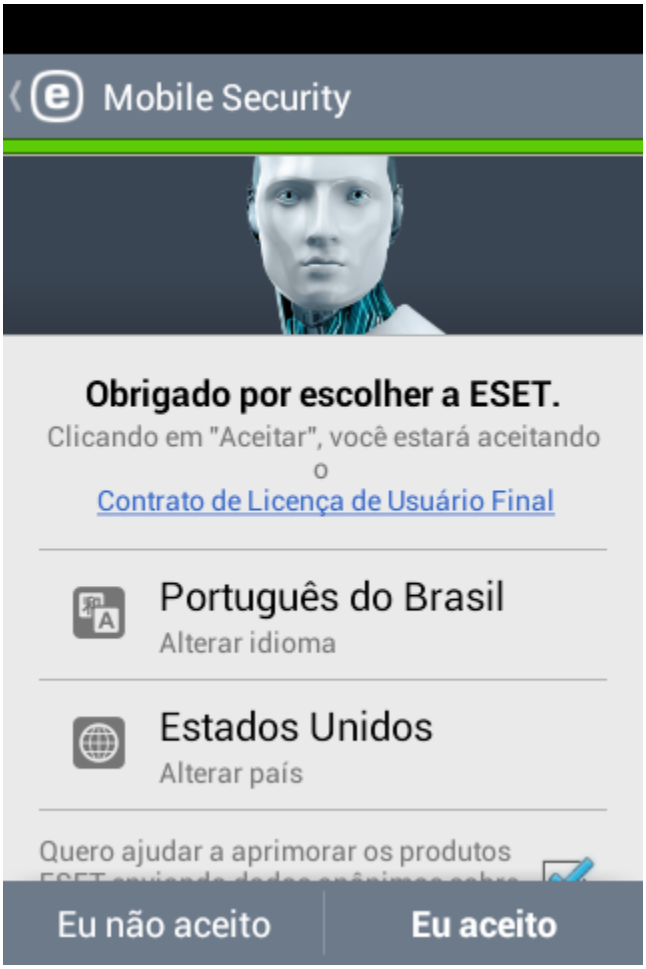
Abra o aplicativo Google Play Store no seu dispositivo Android e faça uma busca por ESET Mobile Security (ou apenas Eset).

Como alternativa, você pode instalar o programa por meio da leitura do código QR a seguir usando seu dispositivo móvel e um aplicativo como QR Droid ou Barcode Scanner:

2.3 Instalação da Amazon

Abra o aplicativo Amazon no seu dispositivo Android e faça uma busca por ESET Mobile Security (ou apenas Eset).

2.4 Assistente inicial



Quando o aplicativo estiver instalado em seu dispositivo, siga os avisos do Assistente inicial:

1. Selecione o idioma que você deseja usar no ESET Mobile Security.
2. Selecione o país onde reside atualmente.
3. Se desejar ajudar a aprimorar os produtos ESET enviando dados anônimos sobre o uso do aplicativo, selecione a opção apropriada.
4. Toque em **Aceitar**. Ao fazer isso você concorda com o Contrato de Licença de Usuário Final.
5. No próximo passo, escolha se deseja participar do ESET Live Grid. Para saber mais sobre o ESET Live Grid, consulte esta seção 8.
6. Toque em **Avançar**.
7. Selecione se você deseja que o ESET Mobile Security detecte Aplicativos Potencialmente Indesejados. É possível encontrar mais detalhes sobre tais aplicativos nesta seção 8.
8. Toque em **Avançar**.
9. Toque em **Finlandês**.

2.5 Desinstalação

Se você deseja desinstalar o ESET Mobile Security, use o assistente de Desinstalação disponível no menu principal ESET Mobile Security em **Configurações** > **Desinstalar**. Se você ativou a Proteção contra desinstalar, você precisará digitar sua senha de segurança.

3. Licença

Após a instalação, o ESET Mobile Security deve ser ativado.

Para abrir a seção **Licença**, toque no ícone Menu na tela principal ESET Mobile Security (ou pressione o botão **MENU** no seu dispositivo) e toque em **Licença**.

Os métodos de ativação podem variar dependendo se você fez o download do ESET Mobile Security do site da ESET, Amazon ou Google Play.

- **Avaliação gratuita** - selecione esta opção se você não tiver uma licença e desejar avaliar o ESET Mobile Security antes de fazer a aquisição. Insira seu **endereço de email** para ativar o ESET Mobile Security por um período limitado. Você receberá um email de confirmação depois que o produto for devidamente ativado. Você só pode ativar uma licença de avaliação uma vez por dispositivo.
- **Ativar aplicativo usando seu nome de usuário e senha** - se você comprou o produto de um distribuidor ESET, recebeu um nome de usuário e uma senha no momento da compra. Insira as informações recebidas nos campos **Nome de usuário** e **Senha**.
- **Ativar o aplicativo utilizando sua Chave de ativação** - se tiver adquirido seu programa com um dispositivo novo (ou como um produto em caixa), você recebeu a chave de ativação no momento da compra. Insira as informações recebidas no campo **Chave de ativação** e então seu endereço de email atual no campo **Endereço de Email**. Seus novos dados de autenticação (nome de usuário e senha) substituirão automaticamente a chave de ativação e serão enviados ao endereço de email que você informou.
- **Comprar licença** - selecione esta opção se não tiver uma licença e desejar adquirir uma. Você será redirecionado para a página do seu distribuidor ESET local.

Cada licença é valida por determinado período de tempo. Depois que a licença expirar, você deverá renová-la (o programa notificará sobre essa necessidade com antecedência).

OBSERVAÇÃO: Durante a ativação, o dispositivo precisa estar conectado à Internet. Será feito o download de uma pequena quantidade de dados.

4. Antivírus

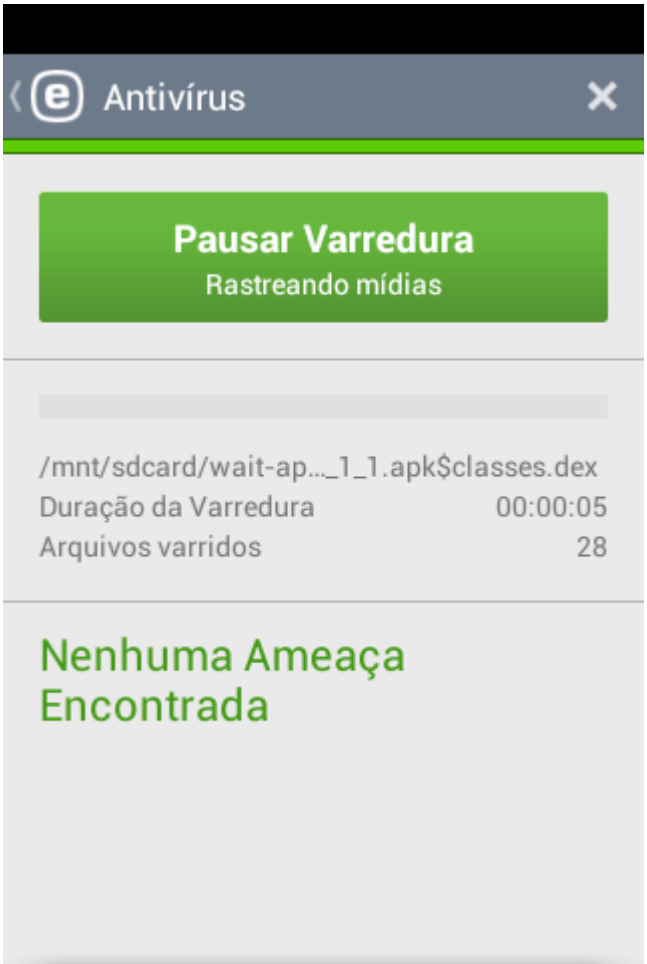
O módulo Antivírus protege seu dispositivo contra códigos maliciosos ao bloquear as ameaças e depois limpando ou movendo tais ameaças para a quarentena.

Rastrear dispositivo

A opção **Rastrear dispositivo** pode ser usada para verificar se há infiltrações no dispositivo móvel.

Alguns tipos de arquivo predefinidos são rastreados por padrão. Um rastreamento completo do dispositivo verifica a memória, os processos em execução e as bibliotecas de links dependentes, assim como os arquivos que fazem parte dos armazenamentos interno e removível. Um breve resumo do rastreamento será salvo em um arquivo de log disponível na seção **Logs**.

Para anular o rastreamento em andamento, toque no ícone.



Nível de Rastreamento

Há três níveis diferentes de rastreamento para escolher:

- **Rápido** - se você selecionar essa opção, o ESET Mobile Security vai fazer o rastreamento apenas dos aplicativos instalados, arquivos DEX (arquivos executáveis para o sistema operacional Android), arquivos SO (bibliotecas) e arquivos ZIP com no máximo 3 níveis de arquivos embutidos.
- **Inteligente** - o rastreamento inteligente vai rastrear o conteúdo do cartão SD e os tipos de arquivos rastreados pelo rastreamento rápido.
- **Profundo** - todos os tipos de arquivos, independentemente de sua extensão, serão verificados tanto na memória interna quanto no cartão SD.

Rastramento Programado

A opção **Rastramento Programado** permite que você execute o rastreamento de Dispositivo automaticamente, em um horário predefinido. Para agendar um rastreamento, toque no botão ao lado da opção **Rastramento Programado** e especifique as datas e horários para que o rastreamento seja iniciado. Por padrão, todos os dias da semana estão selecionados.

Quarentena

O principal objetivo da quarentena é armazenar com segurança os arquivos infectados. Para mais informações consulte a seção Quarentena 8.

Logs de rastreamento

A seção **Logs de rastreamento** traz logs que fornecem dados abrangentes sobre as tarefas de rastreamento concluídas. Mais informações podem ser encontradas neste capítulo 8.

Atualizar Banco de Dados de Ameaças

Por padrão, o ESET Mobile Security inclui uma tarefa de atualização a fim de garantir que o programa seja atualizado regularmente. Para executar a atualização manualmente, toque em **Atualizar Banco de Dados de Ameaças**.

OBSERVAÇÃO: Para evitar a utilização desnecessária da largura de banda, as atualizações são lançadas apenas quando necessário, ou seja, quando surge uma nova ameaça. Embora as atualizações sejam fornecidas gratuitamente com sua licença ativa, a operadora poderá cobrar pela transferência de dados.

As descrições detalhadas das **Configurações Avançadas** de Antivírus podem ser encontradas na seção Configurações Avançadas 8.

4.1 Quarentena

Os arquivos devem ser colocados em quarentena se não for possível limpá-los, se não for seguro nem aconselhável excluí-los ou se tiverem sido falsamente detectados pelo ESET Mobile Security.

É possível consultar os arquivos em quarentena em um log que discrimina o nome e o local original do arquivo infectado junto com a data e a hora em que foram colocados em quarentena.

Para restaurar um arquivo em quarentena para seu local original, toque nele e toque no ícone. Não recomendamos a restauração regular de arquivos na quarentena.

Para remover um arquivo em quarentena permanentemente do dispositivo, toque nele e no ícone.

OBSERVAÇÃO: Se você colocar em quarentena um aplicativo suspeito mas depois escolher instalá-lo, o aplicativo será removido da quarentena automaticamente.

4.2 Logs de rastreamento

Logs de rastreamento são criados após cada rastreamento programado ou rastreamento de dispositivo acionado manualmente.

Cada log contém:

- data e hora do evento
- duração do rastreamento
- número de arquivos rastreados
- resultado do rastreamento ou erros ocorridos durante o rastreamento.

4.3 Configurações avançadas

Banco de Dados de Ameaças com Atualização Automática
Esta opção permite que definir o intervalo de tempo para o download automático das atualizações do banco de dados de ameaças. Essas atualizações são lançadas apenas quando necessário, ou seja, quando surge uma nova ameaça ao banco de dados. Recomendamos que você deixe essa configuração no valor padrão (diariamente).

Proteção em tempo real
Esta opção permite que você ative/desative o rastreamento em tempo real. Este rastreamento é iniciado automaticamente na inicialização do sistema e verifica os arquivos com os quais você interage. Ele verifica automaticamente a pasta *Download*, todos os arquivos de instalação *.apk* e todos os arquivos no cartão SD depois dele ser montado.

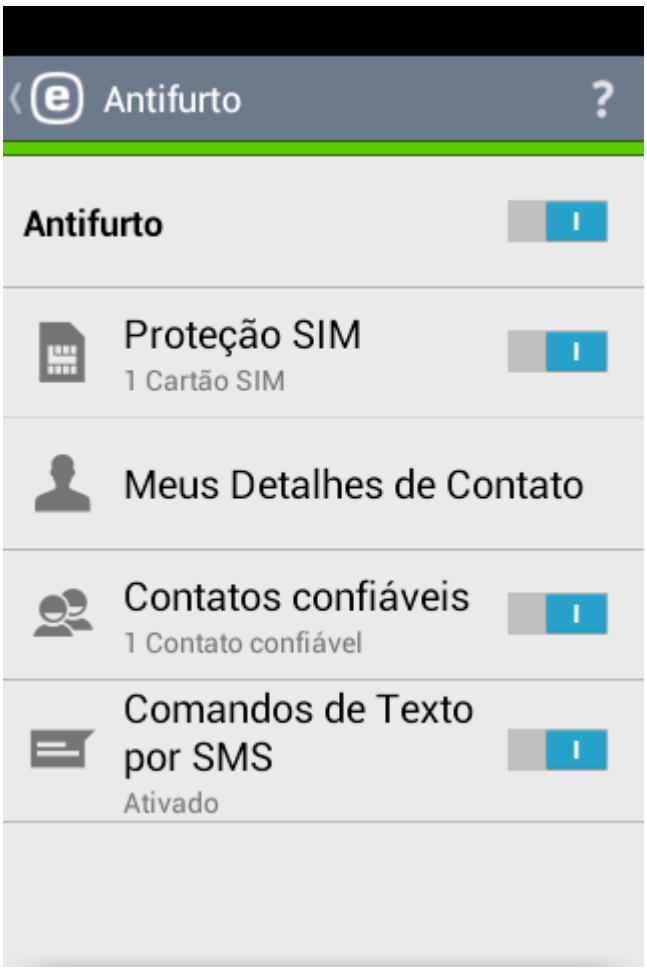
ESET Live Grid
Construído sobre o avançado sistema de alerta precoce ThreatSense.Net, o **ESET Live Grid** é feito para fornecer níveis adicionais de segurança ao seu dispositivo. Ele monitora constantemente os programas e processos sendo executados pelo seu sistema em relação às informações mais recentes coletadas a partir de milhões de usuários ESET em todo o mundo. Além disso, os rastreamentos são processados com mais rapidez e precisão conforme o banco de dados do ESET Live Grid cresce ao longo do tempo. Isso nos permite oferecer proteção proativa e velocidade de rastreamento maiores para todos os nossos usuários. Recomendamos que você ative este recurso. Obrigado pelo seu apoio.

Detectar Aplicativos Potencialmente Indesejados
Um aplicativo indesejado é um programa que contém adware, instala barras de ferramentas, rastreia seus resultados de pesquisa ou tem outros objetivos pouco claros. Existem algumas situações em que você pode sentir que os benefícios do aplicativo indesejado superam os riscos. Por isso o ESET atribui a estes aplicativos uma categoria de risco menor em comparação com outros tipos de software malicioso.

Detectar Aplicativos Potencialmente Inseguros
Há muitos aplicativos legítimos que têm a função de simplificar a administração dos dispositivos conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. A opção **Detectar Aplicativos Potencialmente Inseguros** permite que você detecte tais ameaças. "Aplicativos potencialmente inseguros" é a classificação usada para software comercial legítimo. Essa classificação inclui programas como ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado.

Ação de Solução Padrão
Esta configuração determina uma ação padrão que será realizada após o rastreamento ser concluído e as ameaças serem encontradas. Se selecionar **Remover**, o arquivo infectado será removido. Se selecionar **Quarentena**, o arquivo infectado será colocado em quarentena 8.

5. Antifurto



A funcionalidade Antifurto protege seu dispositivo móvel contra o acesso não autorizado.

Se você perder seu aparelho ou alguém roubá-lo e substituir seu cartão SIM por um cartão novo (não confiável), o dispositivo será bloqueado automaticamente pelo ESET Mobile Security e um SMS de alerta será enviado para o(s) número(s) de telefone definido(s) pelo usuário. Essa mensagem incluirá o número de telefone do cartão SIM inserido no momento, o número IMSI (International Mobile Subscriber Identity, identidade internacional de assinante móvel) e o número IMEI (International Mobile Equipment Identity, identidade internacional de equipamento móvel) do telefone. O usuário não autorizado não terá conhecimento do envio desta mensagem porque ela será automaticamente excluída das sequências de mensagens do seu aparelho. Você também pode solicitar coordenadas de GPS do aparelho perdido ou apagar remotamente todos os dados armazenados no dispositivo.

OBSERVAÇÃO: O recurso Antifurto não funciona em tablets que não suportam mensagens.

Para começar a usar a proteção Antifurto, toque em **Antifurto** no menu principal do programa. Um assistente simples irá guiá-lo através de algumas etapas: habilitar a Proteção contra Desinstalação, adicionar ESET Mobile Security como um Administrador do dispositivo, criar sua própria senha de segurança e criar uma senha para comandos de texto por SMS.

Sua **Senha de Segurança** é necessária para desbloquear o dispositivo, acessar recursos protegidos com senha (por exemplo o Antifurto) e desinstalar o ESET Mobile Security. Sua **Senha para comandos de texto por SMS** é usada para enviar os comandos de texto. Para ler mais sobre comandos de texto, veja esta seção 11.

IMPORTANTE: Escolha suas senhas com cuidado. Para aumentar a segurança e fazer com que suas senhas sejam mais difíceis de adivinhar, use uma combinação de letras minúsculas, maiúsculas e números.

5.1 Proteção SIM

A seção **Proteção SIM** mostra a lista de cartões SIM confiáveis que serão aceitas pelo ESET Mobile Security. Se você inserir um cartão SIM não definido nesta lista, a tela será bloqueada e um SMS de alerta será enviado para seus **Contatos Confiáveis**.

Para adicionar um novo cartão SIM, toque no ícone. Para ler mais, veja esta seção 10.

Para remover um cartão SIM da lista, toque e segure a entrada e toque no ícone.

5.1.1 Adicionando um novo SIM Confiável

Digite um **Nome para o Cartão SIM** (por exemplo, casa, trabalho) e seu número **IMSI** (International Mobile Subscriber Identity). O IMSI (International Mobile Subscriber Identity) normalmente é apresentado como um número de 15 dígitos impresso no seu cartão SIM. Em alguns casos, ele pode ser mais curto.

5.2 Meus Detalhes de Contato

Na seção **Meus Detalhes de Contato** você pode digitar as informações que serão enviadas ao(s) número(s) de telefone predefinido(s) se um cartão SIM não confiável for inserido no seu dispositivo. Digite a descrição do seu dispositivo, um número de contato alternativo (por exemplo, número de telefone residencial ou de trabalho) ou seu endereço de e-mail.

5.3 Contatos confiáveis

Na lista de **Contatos Confiáveis** você pode adicionar ou remover os números de telefone das pessoas que receberão um SMS de alerta se um cartão SIM não confiável for inserido no seu dispositivo. Para adicionar um novo contato confiável, toque em **Adicionar a partir dos Contatos** e selecione um contato da sua lista.

Se a pessoa não fizer parte da sua lista de contato, toque no ícone. Para ler mais, veja esta seção 11.

Para remover um contato da lista, toque e segure o contato e

toque  no ícone.

OBSERVAÇÃO: Se você estiver no exterior, todos os números de telefone inseridos na lista deve incluir o código de discagem internacional seguido pelo número propriamente dito (por exemplo, +1610100100).

5.3.1 Adicionando um novo Contato Confiável

Digite o nome de um contato e seu número de telefone. Caso o contato tenha mais de um número de telefone, o SMS de alerta será enviado para todos os números associados. Se você quiser permitir que este contato redefina sua senha no caso de você esquecê-la, selecione a opção **Permitir redefinição remota da senha**.

5.4 Comandos de Texto por SMS

Comandos SMS remotos (bloqueio, apito, encontrar e apagar) só vão funcionar se os **Comandos de Texto por SMS** estiverem habilitados.

Se você perder seu dispositivo e desejar bloqueá-lo, envie um SMS de bloqueio remoto para seu celular a partir de qualquer outro dispositivo móvel no seguinte formato:
eset lock senha
Troque *senha* por sua senha de segurança. Quando seu dispositivo estiver bloqueado, um usuário não autorizado será obrigado a digitar sua senha para desbloqueá-lo.

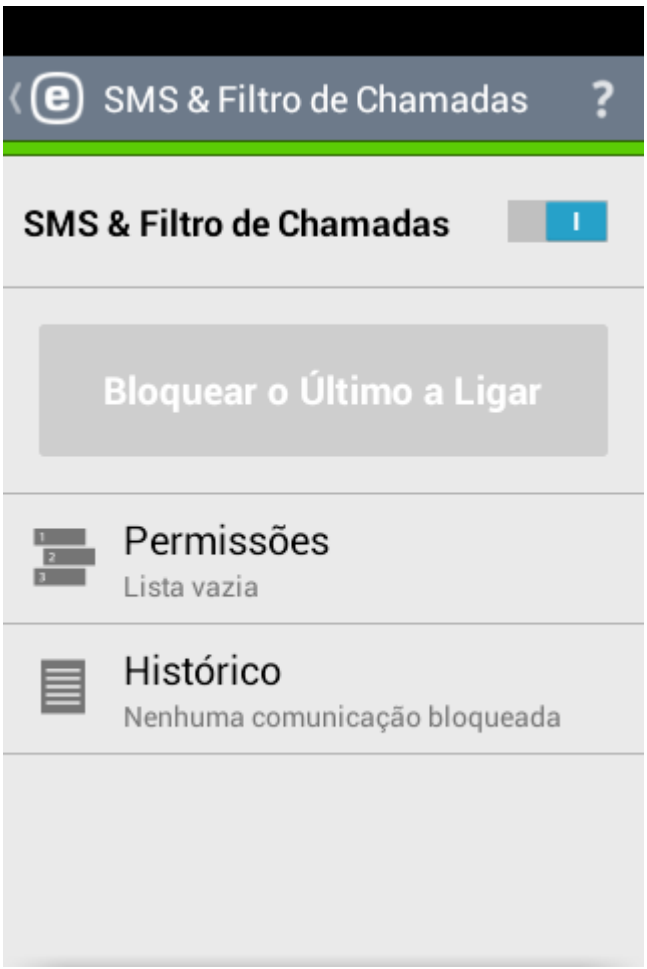
Para bloquear o dispositivo e fazer um som, envie um SMS para seu número de celular da seguinte forma:
eset siren senha

Para solicitar as coordenadas de GPS do seu celular, envie uma mensagem de texto para seu celular ou para o número de telefone do usuário não autorizado (se o cartão SIM já tiver sido substituído) da seguinte forma:
eset find senha
Você receberá uma mensagem de texto com a localização aproximada do seu dispositivo perdido e uma segunda mensagem de texto com as coordenadas de GPS exatas de seu dispositivo incluindo um link para esse local no Google Maps. Para que seja possível receber as coordenadas de GPS, o módulo GPS do aparelho deverá ter sido previamente ativado.

Para apagar todos os dados armazenados no seu dispositivo e todas as mídias removíveis inseridas no momento, envie um SMS de Limpeza Remota para seu aparelho da forma a seguir:
eset wipe senha
Todos os contatos, mensagens, e-mails, aplicativos instalados, sua conta do Google e o conteúdo do cartão SIM serão permanentemente apagados do dispositivo. Se o ESET Mobile Security não estiver definido como o Administrador do dispositivo, somente os contatos, as mensagens e o conteúdo do cartão SD serão apagados.

OBSERVAÇÃO: A senha diferencia maiúsculas e minúsculas. Insira a senha exatamente como ela foi definida durante o assistente de configuração Antifurto.

6. SMS & Filtro de Chamadas



O **SMS e Filtro de Chamadas** bloqueia mensagens SMS/MMS recebidas e chamadas recebidas/realizadas de acordo com as suas regras.

Mensagens indesejadas geralmente incluem anúncios de operadoras ou mensagens de usuários desconhecidos ou indeterminados. O termo *bloquear mensagens* refere-se à transferência automática de uma mensagem recebida para a seção **Histórico**. Nenhuma notificação é exibida quando uma mensagem recebida é bloqueada. A vantagem é que o usuário não é incomodado pelas informações indesejadas, mas, ao mesmo tempo, pode consultar os logs para procurar mensagens que possam ter sido bloqueadas por engano.

OBSERVAÇÃO: O SMS e Filtro de Chamadas não funciona em tablets que não suportam chamadas e mensagens.

Para bloquear chamadas e mensagens vindas do último número de telefone recebido, toque em **Bloquear o Último que ligou**. Isto vai criar uma nova regra de SMS e Filtro de Chamada.

6.1 Permissões

Para adicionar uma nova regra, toque no ícone. Mais informações sobre a criação de uma nova regra podem ser encontradas nesta seção 12.

Se você quiser remover uma entrada de regra existente da lista de **Regras**, toque na entrada e segure e toque no ícone.

6.1.1 Adicionando uma nova regra

Especifique um grupo de números de telefone ou uma pessoa. **Todos os números desconhecidos** vai incluir os números de telefone que não estão salvos na sua lista de contatos. Você pode usar essa opção para bloquear chamadas indesejadas (por exemplo, ligações de telemarketing) ou para evitar que crianças disquem números desconhecidos. A opção **Todos os números conhecidos** diz respeito a todos os números de telefone guardados na sua lista de contatos. **Números restritos** serão aplicados para ligações de pessoas que ocultaram seu número de telefone deliberadamente pelo recurso de restrição de identificação da linha chamadora.

Especifique o que deve ser bloqueado ou permitido:

- chamadas enviadas
- chamadas recebidas
- mensagens de texto (SMS) recebidas ou
- mensagens multimídia (MMS) recebidas

Para aplicar a regra apenas por um tempo determinado, desmarque **Sempre** na parte inferior e selecione as datas e horários em que você quer que a regra seja aplicada. Por padrão, todos os dias da semana estão selecionados. Esta funcionalidade pode vir a calhar se você não quiser ser incomodado durante a noite ou durante o fim de semana.

OBSERVAÇÃO: Se você estiver no exterior, todos os números de telefone inseridos na lista deve incluir o código de discagem internacional seguido pelo número propriamente dito (por exemplo, +1610100100).

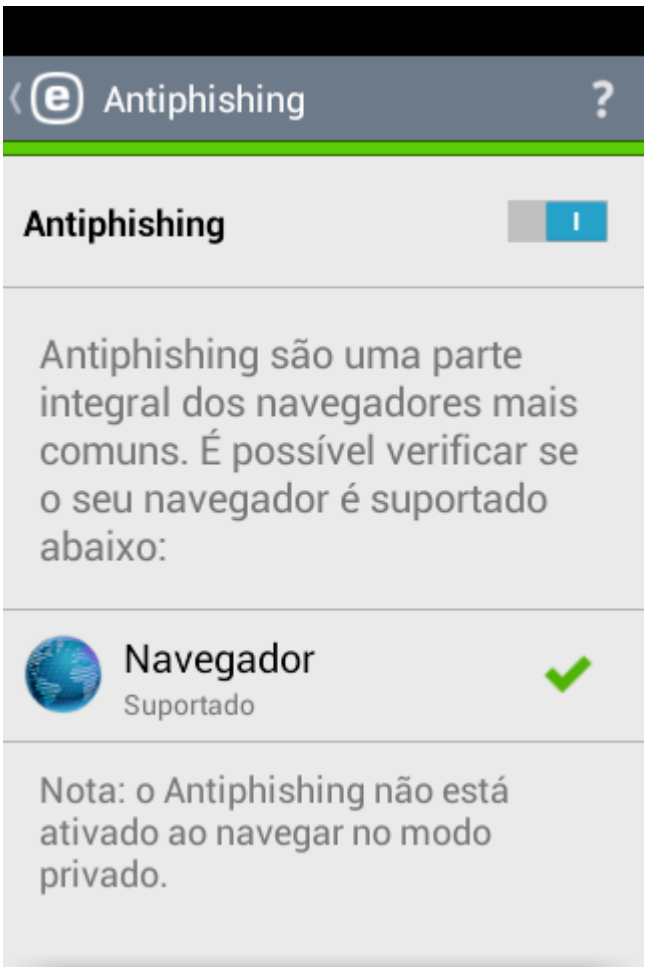
6.2 Histórico

Na seção **Histórico** você pode consultar as chamadas e mensagens bloqueadas ou permitidas pelo SMS e Filtro de Chamadas. Cada log contém o nome do evento, o número de telefone correspondente e a data e a hora do evento. Os registros de mensagens SMS e MMS também preservam o corpo da mensagem.

Se você quiser modificar uma regra relacionada ao número de telefone ou contato que foi bloqueado, selecione a entrada na lista tocando nela e  no ícone.

Para remover a entrada da lista, selecione-a e toque  no ícone. Para remover mais entradas, toque e segure uma das entradas, selecione as entradas que você deseja remover e toque  no ícone.

7. Antiphishing



O termo *phishing* define uma atividade criminal que usa engenharia social (a manipulação de usuários a fim de obter informações confidenciais). O roubo de identidade é utilizado frequentemente para obter acesso a dados confidenciais como números de contas bancárias, números de cartões de crédito, números de PIN ou nomes de usuários e senhas.

Recomendamos que você mantenha ativado o **Antiphishing**. Todos os ataques potenciais de roubo de identidade que vêm de sites ou domínios listados no banco de dados de malware da ESET serão bloqueados e uma notificação de aviso será exibida, informando sobre o ataque.

O Antiphishing pode ser integrado com os navegadores mais comuns disponíveis no sistema operacional Android (por exemplo Chrome ou navegador padrão do Android). A lista de navegadores suportados foi validada antes do lançamento de sua versão instalada do ESET Mobile Security.

Para verificar se o navegador instalado no seu dispositivo é suportado pelo ESET Mobile Security, toque no nome do navegador. O ESET Mobile Security irá verificar a compatibilidade com o navegador atual.

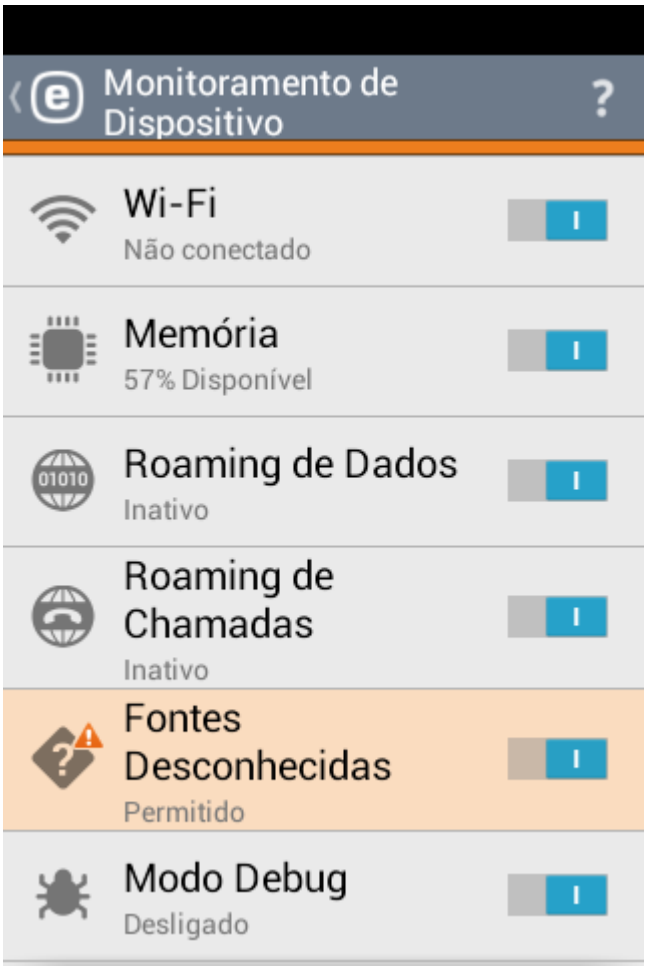
OBSERVAÇÃO: O Antiphishing não irá protegê-lo durante a navegação em modo privado (anônimo).

8. Auditoria de segurança

A **Auditoria de Segurança** ajuda a monitorar e alterar configurações importantes do dispositivo e permissões dos aplicativos instalados para prevenir riscos de segurança.

Para ligar/desligar a Auditoria de Segurança e seus componentes específicos, use estes botões: 

8.1 Monitoramento do Dispositivo

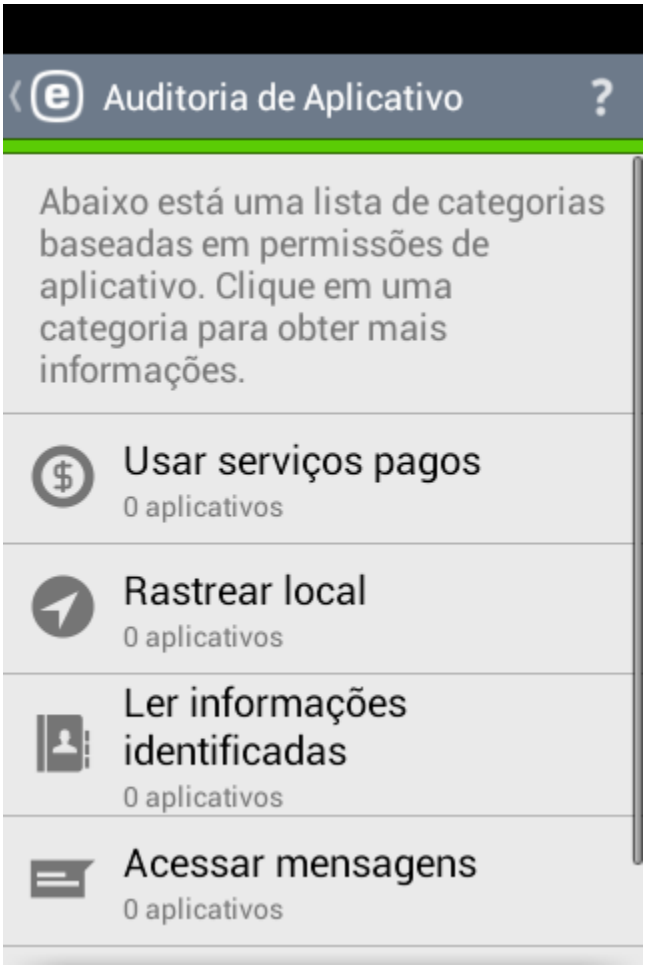


Na seção **Monitoramento do Dispositivo** você pode definir quais componentes do dispositivo serão monitorados pelo ESET Mobile Security.

Toque em cada opção para ver uma descrição detalhada da opção e seu status atual.

Algumas opções como **Fontes Desconhecidas** e **Modo Debug** podem ser alteradas tocando em **Alterar Configurações**. Isso vai redirecioná-lo para a tela de configurações do sistema operacional Android.

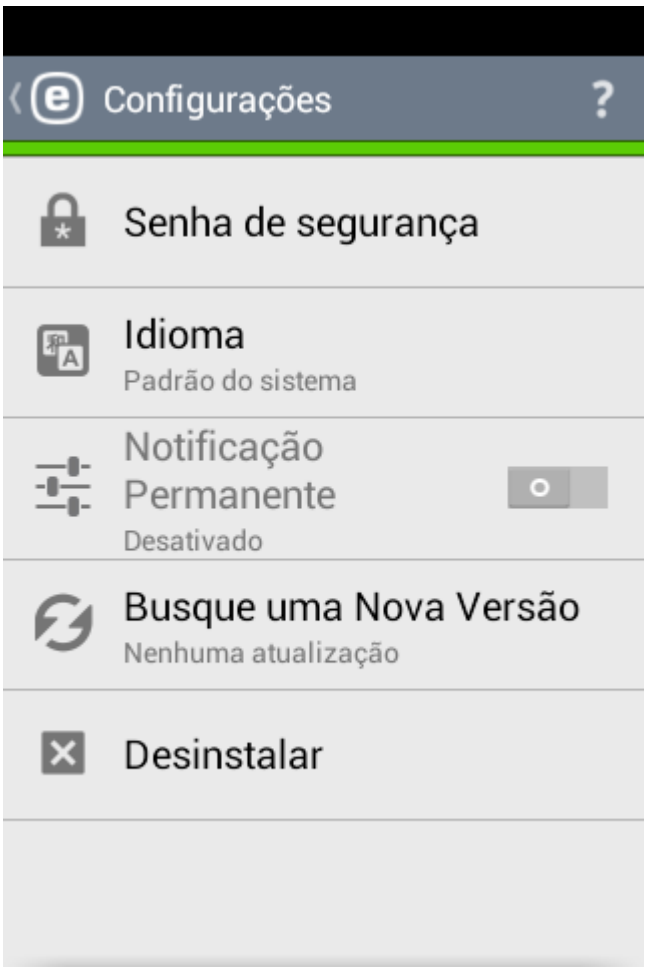
8.2 Auditoria de Aplicativo



Alguns aplicativos instalados no seu dispositivo podem ter acesso a serviços que cobram, rastreiam sua localização ou lêem suas informações de identidade, contatos ou mensagens de texto. O ESET Mobile Security fornece uma auditoria para estes aplicativos.

Na seção **Auditoria de Aplicativo** você pode ver a lista de aplicativos classificados por categoria. Toque em cada categoria para ver sua descrição detalhada. Os detalhes de permissões de cada aplicativo podem ser acessados tocando em um determinado aplicativo.

9. Configurações



Senha de segurança
Esta opção permite que você defina uma nova senha de segurança ou altere a senha existente. Para mais informações consulte a seção Senha de Segurança 16.

Idioma
Por padrão, o ESET Mobile Security é instalado no idioma definido em seu telefone como local do sistema (nas configurações de idioma e teclado do sistema operacional Android). Para alterar o idioma da interface de usuário do aplicativo, toque em **Idioma** e selecione o idioma desejado.

Notificação Permanente

O ESET Mobile Security exibe seu ícone de notificação no canto superior esquerdo da tela (barra de status do Android). Se você não deseja que esse ícone seja exibido, desmarque **Notificação Permanente**.

Busque uma Nova Versão
Para o máximo de proteção, é importante usar a versão mais recente do ESET Mobile Security. Toque em **Buscar uma Nova Versão** para ver se há uma nova versão disponível para download.

Desinstalar
Se você deseja desinstalar o ESET Mobile Security, use o assistente de **Desinstalação**. O ESET Mobile Security e a pasta de quarentena serão excluídos permanentemente.

9.1 Senha de segurança

Sua **Senha de Segurança** é necessária para desbloquear o dispositivo, acessar recursos protegidos com senha (por exemplo o Antifurto) e desinstalar o ESET Mobile Security. O **Lembrete de senha** (quando configurado) exibe uma dica para ajudá-lo a se lembrar da sua senha.

Se você esquecer sua senha, poderá enviar um SMS para seu número a partir do celular salvo na lista Contatos confiáveis 10. Esse SMS deve ter o seguinte formato:
eset remote reset
Sua senha será redefinida. Então você poderá definir uma nova senha.

Se você não tem um Contato confiável definido antes de bloquear seu dispositivo, você pode enviar um pedido de redefinição de senha. Esta opção ficará ativa na tela do seu telefone bloqueado após duas tentativas de senha mal sucedidas. Você receberá um email contendo um código de desbloqueio no seu endereço de email da conta Google ou em um endereço de e-mail definido em **Antifurto** > **Meus Detalhes de Contato**. Digite o código de desbloqueio na tela do seu telefone bloqueado. Quando seu telefone estiver desbloqueado, defina uma nova senha de segurança em **Configurações** > **Senha**.

IMPORTANTE: Escolha sua senha com cuidado. Para aumentar a segurança e fazer com que sua senha seja mais difícil de adivinhar, use uma combinação de letras minúsculas, maiúsculas e números.

10. Atendimento ao cliente

Os especialistas de atendimento ao cliente ESET estão disponíveis para ajudar caso você precise de assistência administrativa ou suporte técnico relacionado ao ESET Mobile Security ou a outro produto de segurança ESET.

Para enviar uma solicitação de atendimento diretamente de seu dispositivo, toque no ícone do Menu  na tela principal ESET Mobile Security (ou pressione o botão **MENU** no seu dispositivo) e toque em **Atendimento ao cliente** > **Atendimento ao cliente**. Preencha todos os campos obrigatórios.

O ESET Mobile Security inclui recursos avançados de registro em log para ajudar a diagnosticar possíveis problemas técnicos. Para fornecer para a ESET um log detalhado do aplicativo, certifique-se que **Log do aplicativo** está selecionado (padrão). Envie sua solicitação tocando em **Enviar**. Especialistas de Atendimento ao Cliente ESET vão entrar em contato com você no endereço de e-mail fornecido.